SHARING THE KNOWLEDGE:

GOVERNMENT-PRIVATE

SECTOR PARTNERSHIPS TO

ENHANCE INFORMATION

SECURITY

Steven M. Rinaldi

INSS Occasional Paper 33

Information Operations Series

May 2000

USAF Institute for National Security Studies
USAF Academy, Colorado

The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. Government. This paper is approved for public release by SAF/PAS; distribution is unlimited.

****

Comments pertaining to this paper are invited; please forward to:

Director, USAF Institute for National Security Studies
HQ USAFA/DFES
2354 Fairchild Drive, Suite 5L27
USAF Academy, CO 80840
phone: 719-333-2717
fax: 719-333-2716
email: james.smith@usafa.af.mil

Visit the Institute for National Security Studies home page at
http://www.usafa.af.mil/inss

TABLE OF CONTENTS

FOREWORD

We are pleased to publish this thirtieth-third volume in the *Occasional Paper* series of the US Air Force Institute for National Security Studies (INSS). This paper, along with Occasional Paper 32, Richard Aldrich's *Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime*, address the context surrounding the question of how the U.S. military responds to the cyber threat facing the American military and society today. Aldrich examines definitional and jurisdictional issues, Constitutional and statutory concerns, and both the necessity and desirability of an international treaty addressing cyberterrorism and computer crime. With or without such a treaty, in this paper Steve Rinaldi examines the issues of partnering and sharing sensitive information across private and governmental sectors as a central requirement of a national risk reduction and management effort in the face of the threat of cyber attack. He makes detailed policy recommendations to overcome the substantial barriers to cross-sector cooperation and enhanced national security. Together these two papers provide fresh thinking and critical perspective on a security threat arena that increasingly captivates the headlines.

About the Institute

INSS is primarily sponsored by the National Security Policy Division, Nuclear and Counterproliferation Directorate, Headquarters US Air Force (HQ USAF/XONP) and the Dean of the Faculty, USAF Academy. Our other sponsors currently include the Air Staff's Intelligence, Surveillance, and Reconnaissance Directorate (XOI) and the Air Force's 39th Information Operations Squadron; the Secretary of Defense's Office of Net Assessment (OSD/NA); the Defense Threat Reduction Agency (incorporating the sponsorship of the Defense Special

Weapons Agency and the On-Site Inspection Agency); the Army Environmental Policy Institute; the Plans Directorate of the United States Space Command; the Air Force long-range plans directorate (XPXP); and the Nonproliferation Center of the Central Intelligence Agency. The mission of the Institute is "to promote national security research for the Department of Defense within the military academic community, and to support the Air Force national security education program." Its research focuses on the areas of greatest interest to our organizational sponsors: arms control, proliferation, regional studies, Air Force policy, information operations, environmental security, and space policy.

INSS coordinates and focuses outside thinking in various disciplines and across the military services to develop new ideas for defense policy making. To that end, the Institute develops topics, selects researchers from within the military academic community, and administers sponsored research. It also hosts conferences and workshops and facilitates the dissemination of information to a wide range of private and government organizations. INSS provides valuable, cost-effective research to meet the needs of our sponsors. We appreciate your continued interest in INSS and our research products.

JAMES M. SMITH
Director

EXECUTIVE SUMMARY

The U.S. military has become increasingly dependent upon the nation's information and communications infrastructures. Concurrently, threats to and vulnerabilities in these infrastructures are expanding, in large part due to structural factors not likely to disappear in the future. To prevail against the increasing threat, the military—and, more broadly, the government—needs to adopt a risk reduction and management program. A crucial element of this risk management program is information sharing with the private sector.

However, substantial barriers threaten to block information exchanges between the government and private sector. These barriers include concerns over release of sensitive material under Freedom of Information Act requests, antitrust actions, protection of business confidential and other private material, possible liability due to shared information, disclosure of classified information, and burdens entailed with cooperating with law enforcement agencies. There is good cause to believe that the government and private sector can overcome these barriers, guided by lessons learned from numerous successful government-private sector information-sharing mechanisms.

This analysis concludes with actions the government should undertake to develop an information-sharing mechanism with the private sector. Key among them are actively engaging the private sector from the onset, determining information requirements, and fostering a partnership based on trust.

ACKNOWLEDGEMENTS

I wish to express my sincere appreciation to several persons who have provided their insights and encouragement to me during this project: Lee M. Zeichner, Esq. (Critical Infrastructure Assurance Office), Bernie Farrell (Manager, National Coordination Center for Telecommuni-cations), Mark Centra (ASD/C3I), Jan Philpot (CERT® Coordination Center), Richard Pethia (CERT® Coordination Center), and Tom Longstaff (CERT® Coordination Center). In particular, the CERT® Coordination Center staff pointed out that *information sharing is not an end in itself, but rather a means to an end (reduced network risk)*, a key point that is often lost in discussions. I am grateful to innumerable others in government and the private sector who have contributed to my thoughts during the past two years while I have participated in, and hopefully contributed to, the federal government's critical infrastructure protection program.

I alone am responsible for the opinions expressed in this paper and any errors or omissions.